

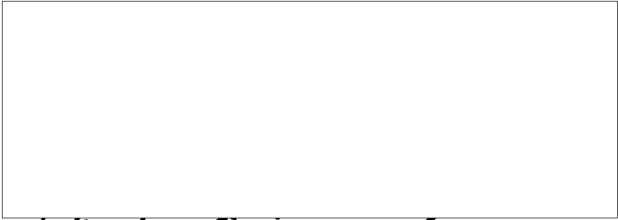
14 NOV 1974

MEMORANDUM FOR: Members of the Computer Security Subcommittee
of the United States Intelligence Board

SUBJECT : Intelligence Community Policy for the
Security of Computer Operations

1. Attached you will find the latest Draft of subject policy. Would you please review and be prepared to discuss same at a meeting of the Subcommittee scheduled for 0930 hours on 22 November 1974. The length of this meeting will depend on the work needed to produce an acceptable "Final" Draft for subsequent coordination at the Subcommittee level. It is the goal of the Acting Chairman to accomplish this at the 22 November meeting.

2. It is envisioned that the memorandum to accompany this "Final" Draft will indicate our intention to supply various annexes covering specific issues: e.g., The Intelligence Community Policy for the Release of Magnetic Storage Media; Analysis, Test, and Evaluation procedures, and the like.


✓ Acting Chairman
Computer Security Subcommittee

STAT

Attachment

CENTRAL INTELLIGENCE AGENCY
WASHINGTON, D.C. 20505

19 December 1974

MEMORANDUM FOR: Member, Computer Security Subcommittee

SUBJECT : Final Draft - Intelligence Community
Policy for the Security of Computer
Operations

1. Attached you will find the final draft of subject paper agreed to by those in attendance at the last meeting of the Subcommittee, 16 December 1974. As the Minutes of that meeting will show, this draft is scheduled to be forwarded to the Security Committee for initial coordination action.

2. This final draft will be formally forwarded to the Chairman, Security Committee on 7 January 1975. You are requested to notify the CIA member of your comments and/or concurrence in this action prior to that time. This may be done in writing or by telephone,

[Redacted]

STAT

[Redacted]

STAT

✓ CIA Member
Computer Security Subcommittee

Attachment



DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

UNITED STATES ARMY INTELLIGENCE SYSTEMS SUPPORT DETACHMENT

REPLY TO
ATTENTION OF:

DAMI-SS

8 July 1974

*File CSS
IC Policy
Computer Sec*

MEMORANDUM FOR: CHAIRMAN, COMPUTER SECURITY SUBCOMMITTEE (CSS),
SECURITY COMMITTEE (SECOM), USIB

SUBJECT: Preliminary Review of Draft Intelligence Community Policy
Paper on Computer Security

1. Reference draft paper, undated, subject: Intelligence Community Policy and Procedures for the Maintenance of Computer Security. (Inclosed)

2. The undersigned has reviewed referenced paper as requested by you during the 31 May 1974 CSS meeting. Review of the draft was made strictly on the basis of the subjects included (or not included) in the paper. No attempt was made to evaluate the policies or the wording of the paper; that will require considerably more detailed analysis.

3. The following comments and recommendations reflect the undersigned's views as to what should (and should not) be included in an IC policy paper on computer security:

a. If at all possible, the paper should not address the "privacy" area. This is a highly emotional issue at the present time and involves far more than just computer security (e.g., the question of what kinds of personal data should be collected and maintained on US citizens). If this paper addresses "privacy", it may complicate and lengthen the coordination process.

b. At a minimum, the following terms should be defined in the paper:

ADP System Security ✓	Acceptable Risk
Compartmented Mode	Dedicated Mode
Collateral Data	Sensitive Compartmented
Controlled TOP SECRET	Information (SCI)
Environment	Multilevel Security Mode
Central Computer Facility	
Designated Approving Authority	Systems Accreditation

c. Security responsibilities should be placed at the beginning of the paper. This section should be very explicit about who accredits ADP systems for multilevel security and compartmented modes of operation.

DAMI-SS

SUBJECT: Preliminary Review of Draft Intelligence Community Policy
Paper on Computer Security

The responsibilities of the ADP System Security Officer (ADPSSO) and the Terminal Area Security Officer (TASO) should be covered in more detail.

d. The security mode options for processing SCI should be discussed in considerable detail (i.e. dedicated mode, compartmented mode, waiver basis).

e. Recommend use of matrix charts to reflect at a glance:

(1) Who accredits ADP systems for the various security modes.


(2) Security requirements for the various security modes.

f. The paper should discuss risk analysis steps/techniques. This would help ADPSSO's and ADP managers in their efforts to assess and define the risks involved in processing sensitive information in their particular systems, under various security modes of operation.

g. Recommend the detailed section on Tempest/Red-Black requirements be left out of the paper. These are covered adequately in other directives and regulations and only tend to lengthen this paper unnecessarily. It is sufficient for this paper to reference those documents which outline national policy on Tempest/Red-Black requirements.

h. In addition to the section on the Storage, Control and Release of Storage Media, the paper should include a section which describes the procedures to be followed to sanitize storage media, prior to reuse within protected environments (e.g. clearing core after a period of processing SCI, and before TOP SECRET terminals are connected to the system for a period of TOP SECRET processing).

1 Incl
as


JOHN C. KARP, JR.
MAJ, MI
Army Member, CSS

FILE DESIGNATION

IC COMPUTER

CONCURRENCES

SEC. POLICY

CS

SC

SAC

IG

CC

DS

DDP

DE

AA

DC

DI

DT

U-65,025/DS-6C3 [] /25 Jan 74/pca

25 JAN 1974

MEMORANDUM FOR THE CHAIRMAN, COMPUTER SECURITY SUBCOMMITTEE,
SECURITY COMMITTEE, USIB

SUBJECT: Intelligence Community Computer Security Policy Paper

The DIA Computer Security Subcommittee (CSS) member has reviewed subject paper as requested. The draft paper, as written, is essentially a "cut and paste" compendium of the relevant portions of DoD Directive 5200.23 and its companion manual. This foregoing fact was acknowledged and discussed at the 18 January 1974 CSS meeting. Now that a "straw man" of the paper has been developed, we believe it would be prudent to proceed as follows: obtain CSS agreement and approval of an outline that provides the organization and structure of the paper; clearly define the scope, applicability, objectives and authority for the paper; and, once this has been accomplished, the chairman would then task individual CSS members to draft appropriate sections of the paper. After all sections of the draft are completed, the CSS would collectively approve the paper. Accordingly, DIA recommends that the CSS adopt the attached outline which we believe will provide the necessary framework for the paper.

1 Enclosure

Proposed Outline - Intelligence MAJ, USA
Community Policy for the Security DIA Member
of Automatic Data Processing Computer Security Subcommittee
Systems and Networks

STAT

STAT

RETURN FOR FILING TO:

Page Denied

Next 3 Page(s) In Document Denied

INTELLIGENCE COMMUNITY POLICY FOR THE
SECURITY OF COMPUTER OPERATIONS

I. GENERAL

A. Purpose: To establish a uniform Intelligence Community comprehensive computer security policy.

B. Authority: This policy is established by the Director of Central Intelligence under his responsibility for the protection of sensitive intelligence sources and methods.

C. Objectives:

1. To establish a uniform security policy for the processing of intelligence information in computers and related information processing techniques, at the same time allowing flexibility in its implementation where possible.
2. To define computer security requirements on a Community basis.
3. To outline optional methods for addressing computer security issues where possible.
4. To reference requirements applicable to the Intelligence Community which are imposed "externally" by statute, Executive Order, etc.
5. To be consistent with DoD regulations, such that although the requirements may vary, they do not contradict one another.
6. To serve as overall guidance for Intelligence Community members not having the benefit of another policy direction in computer security.

D. Applicability

1. This policy applies to the processing of all intelligence information, including all types of sensitive compartmented information.
2. It applies not only to the Intelligence Community, but also to other Government agencies and to contractors where intelligence information is processed.
3. Optionally, within the Intelligence Community, individual USIB members may determine that it applies not only to the processing of intelligence information, but also to the processing of other classified material.
4. Although this policy does not in an authoritative sense dictate requirements for the processing of restricted data and other limited distribution material, it references and is consistent with such requirements, i.e., unless specifically stated to the contrary, this policy is sufficiently demanding to be equal to or greater than the security requirements for the processing of restricted data and such other limited distribution material.

E. Supersession: This policy supersedes and replaces DCID No. 1/16, Annex E of DCID 6/3, et al (spell out)

F. References:

1. DCID No. 1/7
2. DCID No. 1/14
3. Executive Order 11652 and its implementing National Security Council Directive
4. Intelligence Community physical security standards for sensitive compartmented information

G. Definitions: (to be identified)

F. Effective Date

II. SECURITY, PRIVACY AND COMPARTMENTATION IN THE COMPUTER ENVIRONMENT

- A. The Problem: Discussion of the fact that the state-of-the-art cannot guarantee in an absolute sense compartmentation of data in resource-sharing systems -- thus the security approach to the problem must be from an inhibiting standpoint, i.e., recognizing that technical penetration is possible, security countermeasures must discourage attempts and/or make them more difficult. Further, restriction of the computer environment and other traditional security techniques play a major role in computer security.
- B. Decision to Computerize: In view of the lack of absolute protection, careful consideration must be given to the introduction of sensitive data to resource-sharing systems. The data sensitivity must be weighed against the degree of protection possible.
- C. Need for Computer Security Education: Members of computer operations and users of computer systems must be aware of the security vulnerabilities associated with system use; secondly, both must

recognize their responsibilities for the security of the overall system. An error by one user may endanger the data of all users.

- D. The Privacy Threat: While security or need-to-know can be violated for espionage reasons, data requiring privacy protection is threatened out of curiosity and less important motivations than espionage.

III. POLICY

- A. The contents of this paper are established as Intelligence Community policy requirements.
- B. Their implementation will be effected through individual USIB members.
- C. Waivers of the requirements in this paper for just reasons are permitted by USIB members or their designees with the following exceptions:
1. In cases involving the storage and processing of sensitive compartmented information, waivers may be granted by the USIB member alone.
 2. In cases involving inter-Agency networks or bilateral computer links, waivers will be permitted

only when all parties involved in the network or bilateral link agree (the agreement of network or link participants outside of the Intelligence Community is not necessary in these cases).

IV. ENVIRONMENTAL SECURITY REQUIREMENTS

- A. The security classification and sensitivity of data processed or stored in computers predicate the basic physical, personnel, procedural and other security requirements for the environment of processing.
1. Hierarchial National Clearance Level: TOP SECRET, SECRET, CONFIDENTIAL (attention should be called to the significant investigative and adjudication differences existing between SECRET and TOP SECRET clearances.
 2. Dissemination controls as defined by DCID No. 1/7, especially "No Foreign Dissemination" and "Controlled Dissemination".
 3. Dissemination controls associated with the various types of sensitive compartmented information.

4. Dissemination controls applicable to restricted data, formerly restricted data, cryptographic material, and other such information, whose security controls are established outside the Intelligence Community but apply uniformly throughout the Community.
5. Special compartmentation controls established by an individual Agency for compartmentation purposes, but not on a Community basis.

B. The basic formula for defining access requirements is the need for the users clearance level and the site clearance level to meet the classification and control levels associated with the data.

C. Physical security and access control requirements - what are they and how may they be accomplished in terms of:

1. Computer centers
2. Terminal areas
3. Communications Links

D. TEMPEST Requirements

V. SECURITY PARAMETERS FOR OPERATION

A. Dedicated Environment:

1. Computer system or center without remote terminal devices.
 2. Remotely accessed systems
- B. Computer systems operated in varying security modes on a timed or scheduled basis.
 - C. Resource-sharing batch environment without remote access.
 - D. Resource-sharing remotely accessed computer systems (this is where DCID No. 1/16 should be spelled out).
 - E. Networks

VI. HARDWARE AND SOFTWARE ISSUES

- A. The use of inhibiting features and techniques, e.g., passwords, authenticators, audit trails.
- B. Continuing controls over software and programmers.
- C. Access to maintenance, vendor and contractor personnel (including TEMPEST considerations).

VII. COMMUNICATIONS

- A. Encypherment
- B. Hard wire or protected grid standards.

VIII. SECURITY RESPONSIBILITIES

- A. USIB Members

- B. Computer managers
- C. Programmers
- D. Users
- E. Network and inter-Agency links

IX. SYSTEM SECURITY ANALYSIS, TESTING AND EVALUATION (see established guidelines)

X. DISASTER PREVENTION AND CONTINGENCY BACK-UP PLANNING
(see CSS paper, already promulgated)

✓ XI. SECURITY LABELS
A. External (including requirement for marking output).
B. Internal (discussion, they are needed and how they may be implemented).

XII. STORAGE, CONTROL, AND RELEASE OF STORAGE MEDIA (point out that data storage is no more encyphered than morse code).

- A. Storage and Controls (discuss libraries, receipting procedures, etc.).
- B. Release from classified Control (the paper just promulgated).

- C. "Downgrading" for Operational Needs, i.e., overwriting for other than release purposes such as between varying security modes of operation.

✓XIII. USER SECURITY INDOCTRINATION

NOTE: The document must also include an index and Table of Contents